STATEMENT OF THE HONORABLE WM. LACY CLAY AT THE HEARING ON COMPUTER SECURITY

SEPTEMBER 17, 2003

Thank you Mr. Chairman for calling this hearing. I would like to reiterate two points that I made at last week's hearing. First, the government should use its power in the computer software market place to acquire safer software. Second, software vendors should be more aware of the security configuration of the software they produce. Let me briefly elaborate on these two points.

The federal government spends billions each year on computer hardware and software. Those purchases have a strong influence on what gets produced and sold to the public. The federal government can use its market power to change the quality of software produced, by only buying software that meets security standards. The result will be an increase in the security of all software, and better protection for the public.

This is a simple formulation. The government doesn't have to regulate software manufactures. It only has to use its position in the market place.

Mark Forman, the former federal CIO and regular witness before this Subcommittee, incorporated an idea similar to this when he developed the Smart-Buy program. Mr. Forman realized that federal agencies were buying the same software over and over again. Each agency was paying a different price for the same software, and the federal government was getting little or no leverage out of its position in the market place. No business would operate like that.

I believe we should build on Mr. Forman's idea to buy, not cheaper software, but better software. I hope the new CIO, Karen Evans, will work with the Subcommittee to incorporate this concept into the Smart Buy program.

We don't have to wait for computer companies to develop new security procedures. There are some steps that can be taken very quickly to improve computer security. We saw this earlier this year when Microsoft began shipping software that was configured differently.

The story Microsoft tells is that the company realized that it was shipping software with all the gates open. Good computer managers systematically went through the software, closing gate after gate. Those with less training left the gates open, and the hackers walked in.

Shipping software with secure configurations should be a first priority for all computer companies.

I look forward to the testimony today, and I hope that our witnesses will consider my suggestions and provide the committee with their comments on them.

Thank you Mr. Chairman.